BY ORDER OF THE COMMANDER
433 AIRLIFT WING

433 AIRLIFT WING INSTRUCTION 31-401
12 DECEMBER 2008

Security

INFORMATION SECURITY PROGRAM (ISP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 433 SFS/SFA

Certified by: 433 AW/CC (Brig Gen John C. Fobian)

Pages: 12

This instruction implements Air Force Policy Directive (AFPD) 31-4, *Information Security*. This instruction extends the guidance of Air Force Instruction (AFI) 31-401/Air Force Reserve Command (AFRC) Supplement 1, *Information Security Program Management*, AFI 31-501, *Personnel Security Program Management* and Department of Defense (DoD) 5200.1-R, *Information Security Program*. It provides guidance and procedures on responsibilities of all 433 Airlift Wing (AW) Organizations; specifically all staff agency chiefs, security managers (SM), security monitors, and Top Secret Control Officers (TSCO). The 37 Security Forces Squadron/ Personal and Information Security Section (SFS/S5IP) provides information security oversight and personnel security investigation (PSI) support to 433 AW and submits all PSIs to the Office of Personnel Management (OPM). Each commander/director/staff agency chief is responsible for ensuring assigned personnel comply with DoD 5200.1-R, AFPD 31-4, AFI 31-401/AFRC and Air Education and Training Command (AETC) Supplement, and this Instruction. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force Information Management Tool (AF IMT) 847, *Recommendation for Change of Publication*; route AF IMTs 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/.

1. Appointments and Responsibilities.

1.1. Commander/Staff Agency Chiefs will:

1.1.1. As the responsible officer in charge of the Information Security Program, appoint in writing a Primary and Alternate SM to manage the Information and Personnel Security

Programs. The unit Information Security Program Manager (ISPM) should be a full time employee of the organization. Larger units/sections are encouraged to appoint security monitors at each section to assist the SM. Forward the original appointment letter to 37 SFS/S5IP and a copy to 433 Security Forces Squadron/ Security Forces Administration (SFS/SFA). Ensure SM receives training within 90 days of appointment and attend refresher training annually. The security manager training is conducted by 37 SFS/S5IP.

1.1.2. Designate someone in writing to conduct the semi annual Information Security Program Self Inspection. Security Managers cannot conduct their own self-inspections. File a copy with the final report in your security manager handbook. Inspector uses the localized Security Managers checklist to complete the inspection for cleared or uncleared accounts. Self Inspections are conducted 6 months after the initial program review conducted by 37 SFS/S5IP.

1.1.3. Designate a Primary and Alternate TSCO and identify personnel who are authorized to review Top Secret material.

1.1.4. Designate in writing, Safe/Classified Custodians and those who have access to safe combinations and personnel to perform end of day security checks utilizing Standard Form (SF) 701, *Activity Security Checklist.*

1.1.5. Review position codes in the Unit Manpower Document (UMD). Review Joint Personnel Adjudication System monthly to ensure clearance eligibility & access requirements are consistent with mission needs. Document this review and file in the SMs handbook.

1.1.6. Designate in writing, personnel authorized to receive classified material and forward the original letter to the 433 Communications Flight/Information Systems Flight (CF/SCB) and 433d Airlift Wing/Command Post (AW/CP). Designate in writing personnel authorized to open the inner wrappers of classified material and who can have access to classified material. Maintain file copies in the unit security manager's handbook.

1.2. SM will:

1.2.1. Maintain a SM's handbook as outlined in the AFI 31-401, Air Education Training Command (AETC) Sup 1, Para 1.3.6.10 and 1.3.6.11.

1.2.2. Develop Internal Security Operating Instructions (OIs) and include them as part of the unit initial indoctrination and recurring training programs.

1.2.3. A knowledgeable person must be assigned to conduct self-inspections. Security managers will not conduct self-inspections within their known directorate/unit; however, they are normally the most qualified individuals to inspect programs outside their directorate/unit and commanders/staff agency chiefs are encouraged to utilize them in that role. Monitor the inspection and ensure the commander reviews and endorses the report, and forward a copy of the report with identified corrective action to the ISPM. Maintain the last two self-inspection reports in the SM's handbook.

1.2.4. Ensure SF 312s, *Classified Information Nondisclosure Agreement*, are updated in Joint Personnel Adjudication System (JPAS), and forwarded to Headquarters Air Reserve Personnel Center Personal Office (HQ ARPC/DSMPM) 6760 E. Irvington Place #4450, Denver, CO 80280-4450.

1.2.5. Ensure that personnel having access to TOP SECRET information are given the oral attestation prior to having access.

1.2.6. Have access to required publications for administering the security program.

1.2.7. Attend quarterly security manager meetings sponsored by the host base, and ensure the information received is disseminated throughout the unit.

1.2.8. Establish and maintain an aggressive and recurring security-training program in accordance with AFI 31-401, *Information Security Management Program*, Chapter 8 and attachment 7. The training as a minimum should include Initial Security Education Orientation for cleared and uncleared personnel, Operation Security (OPSEC), North Atlantic Treaty Organization (NATO) Training, and Continuing and Refresher Training. Training will be conducted via the Aeronautical Data Link System (ADLS) Website under Total Force Awareness Training and Information Protection Training.

1.2.9. Ensure authorized personnel conduct Foreign Travel Briefings.

1.2.10. Ensure computer security officers are assigned to the unit.

1.2.11. Coordinate restricted area badge and AF Form 2586, *Unescorted Entry Authorization Certificate*, issues with 433 SFS/SFA and 37 Security Forces Squadron/Pass and Registration Section (SFS/S5B).

1.2.12 SMs will develop and maintain a list of security containers, vaults, and secure rooms located in their organization and include in their security manager's handbook. This list will include make, Identification (ID) number, lock type, and location.

2. Classification or declassification of classified material or information:

2.1. 4 Air Force/Commander (AF/CC) has been designated as a Secret Original Classification Authority (OCA). The authority to originally classify information will be exercised sparingly and only when no promulgated classification guidance exists.

3. Classification challenges:

3.1. All personnel must challenge classification decisions, which they believe, are improper. If information is received which is believed to be improperly classified, or an overly restricted period of continued classification has been assigned, the ISPM and security manager will be contacted.

3.2. The classified information being challenged will be safeguarded at the highest level of classification. If the information is SECRET and the challenge is for downgrading to CONFIDENTIAL, the information must still be safeguarded as SECRET until the challenge has been resolved.

3.3. The ISPM and SM will ensure challenges are acted upon within thirty (30) days.

4. Marking Classified Information:

4.1. The originator of classified information is responsible for proper application of Classification markings. The ultimate responsibility rests with the approver or signer of the document or material.

4.2. Those who prepare classified documents are strongly encouraged to consult with their respective SM and review DoD 5200.1-R, Chapter 5, and the Information Security Oversight Office's Marking Classified Nation Security Information Book.

5. Safekeeping and Storage:

5.1. Offices storing small numbers of classified documents that do not warrant an entire Security container (approved General Services Administration (GSA) safe) may request courtesy storage from another office. In this case, a letter of agreement between the two offices is maintained in the safe with the documents. Additionally, the documents must be separated from the safe contents by placing them in a sealed envelope/container.

5.2. Safe Custodians. The persons listed on the SF 700, *Security Container Information*, are considered safe custodians. Safe custodian responsibilities:

5.2.1. Ensure safe combinations are changed as required.

5.2.1.1. Combinations are changed when placed in use; whenever an individual knowing the combination no longer requires access; when the combination has been subject to compromise; at least every 2 years; or when taken out of service.

5.3. Report container malfunction to 37 Civil Engineer Squadron (CES) customer service desk.

5.4. Ensure all documents placed in the safe are properly marked.

5.5. Ensure safe contents are identified in unit office file plans. Personal "work files" of classified information are strongly discouraged but not prohibited. When necessary, these work files should be limited to specifically labeled folders and stored separately from the contents identified in the file plan.

5.6. Become familiar with Technical Order (T.O.) 00-20F-2, *Inspection and Preventative Maintenance Procedures for Classified Storage Containers*, requirements.

5.7. Properly mark each safe with an easily identifiable number (for example, XP-01) permanently attached to the exterior so it can be identified after natural disasters.

5.8. Emergency protection and removal of classified material:

5.8.1. The possibility of fire, civil disturbance, terrorist activity, or natural disaster at Lackland Air Force Base (AFB), Texas (TX) requires development and possible implementation of special procedures for safeguarding and emergency removal of classified material to preclude the material from falling into unauthorized hands. A situation may develop that requires higher headquarters, 4th AF/CC, 433 AW/CC or a designated representative to direct implementation of emergency protection or removal of classified material.

5.8.2. Procedures:

5.8.2.1. Upon notification of emergency removal of classified material implement the following emergency procedures:

5.8.2.2. Remove all classified from security containers and computers.

5.8.2.3. Place the classified material in a large envelope(s), boxes, or appropriate container and mark same, using the highest classification of the contents therein. If time permits accomplish accountability with records/receipts.

5.8.2.4. Safeguard the classified material and wait for further instructions from the 433 wing commander or designated representative.

5.8.2.5. Upon notification of emergency evacuation of classified material, transport the classified material to the location designated by the 433 AW/CC, installation commander, or their designated representative for evacuation.

5.8.2.6. Upon notification of termination of emergency protection/evacuation procedures:

5.8.2.7. Retrieve the classified material from the designated location and return it to its proper storage area.

5.8.2.8. Inventory all classified material prior to returning it to the security container.

5.8.3. In case of fire or natural disaster (tornado, hurricane, earthquake, etc), which results in damage to the building, 433 AW/CC or his designated representative will manage available personnel resources to ensure classified material within the building is protected.

5.8.4. Order of Priority when removing classified:

5.8.4.1. First Priority. Top Secret

5.8.4.2. Second Priority. Secret

5.8.4.3. Third Priority. Confidential.

6. Destruction of classified material:

6.1. Destruction of classified material must be approved by the unit commander, SM, or classified custodian. Classified material belonging to 433 AW can be destroyed by using the unit's approved cross-cut shredding machine located in the 433 AW/CP.

6.2. Annual "Clean Out" Day. The annual cleanout day for 433 AW is the first duty day in August.

7. Transmitting Classified Materials:

7.1. 433 CF/SCB is responsible for processing incoming and outgoing distribution.

7.2. Protect all first class, registered, certified, and Federal Express (or whoever holds current GSA contract), mail as classified information until opened.

7.2.1. Accountable mail received with the incorrect or improper address is referred to the respective commander/staff agency chief. In these cases, the commander/director or SM opens the container to determine the proper addressee. The receipt and container are annotated with the appropriate address before forwarding.

7.3. Removal of Classified Documents from HQ 433 AW (On Base):

7.3.1. Commanders/staff agency chiefs or supervisors approve appropriately cleared personnel to remove classified information from the work area for the following purposes:

7.3.1.1. Routine destruction at the base destruction facility.

7.3.1.2. For official duties on Lackland AFB for hand carrying classified documents the following will be accomplished: obtain supervisor's permission to remove/pick-up the classified material from the workplace, attach the appropriate cover sheet, that is, SF 704, *Secret* (Cover Sheet), or SF 705, *Confidential* (Cover Sheet), and enclose the material in an outer container such as a sealed envelope, folder (closed with a lock, tie, or Velcro), briefcase, zipper bag, etc. **NOTE:** Classified markings must not appear on the outer container.

7.4. Removal of Classified Documents from HQ 433 AW (Off Base): **NOTE:** Within AFRC, removing classified documents/equipment from designated work areas to work on at home is strictly prohibited.

7.4.1.1. For transmission off the installation see DoD 5200.1-R and AFI 31-401.

7.4.1.2. Personnel authorized to remove classified information must be briefed on their responsibilities for protection of classified by their supervisor or SM. This briefing can be annotated on DD Form 2501, *Courier Authorization* (Accountable), or letter.

7.4.1.3. Additional written authorization is required when traveling by aircraft. Consult with your SM and International Security Program (ISP) directives listed above.

8. Reporting a security incident:

8.1. The unit commander and unit security manager will be notified immediately when classified material is compromised, suspected of being compromised, or administratively mishandled and will immediately notify the 37 SFS/S5IP for action on the first duty day if the incident happens on a weekend.

8.2. The unit commander will appoint, in writing, a disinterested Non-Commissioned Officer (NCO) (E-7 or above), a commissioned officer or a civilian employee (Grade Skill Level (GS-7) or above) to conduct inquires or investigations into the events surrounding the suspected violation per AFI 31-401. Provide a copy of the appointment letter to 37 SFS/S5IP. The inquiry/investigation report will be completed within 10 working days and forwarded to 37 SFS/S5I . If the investigation official needs more time, he/she will, in writing, request additional time from the 433 AW/CC and forward this request to 37 SFS/S5IP.

8.3. Security Violation Involving Electronic Mail (E-mail).

8.3.1. Once there is suspected security violation involving e-mail, contact the network system administrator, network control center, OPSEC Manager and 37 SFS/S5IP.

8.3.2. Comply with the requirements outlined by the network system administrator, network control center and assist the inquiry official during their investigation.

9. Automated Information Systems (AIS):

9.1. Computer systems must be approved by the designated approving authority prior to processing classified.

9.2. All removable AIS and word processing media are marked externally with the highest overall classification contained therein via SF 706, *Top Secret* (Label); SF 707, *Secret* (Label); or SF 708, *Confidential* (Label).

9.3. Sections using Global Command Control Systems (GCCS) to produce classified documents will log all printed documents on an AF Form 3137, *General Purpose* (11”x 8 ½”), to ensure accountability. All documents will be protected and destroyed in accordance with DoD 5200.1-R. Once documents are destroyed record their destruction date on the AF Form 3137.

10. Personnel Security:

10.1. The SM will monitor the Personnel Security Program to ensure that a current unit JPAS Eligibility & Access Report is maintained in the SM Handbook.

10.2. For newly assigned personnel, the SM will conduct initial security briefings and check JPAS to validate security clearances and past security clearance history.

10.3. Traditional Reservists submit required paperwork to the authorized requestor within 3 Unit Training Assembly (UTA)s. All other investigations must be completed within 30 days of the initial notification, but the goal is 14 days. Failure to submit required paperwork on time is justification to establish a Security Information File (SIF) and suspend access to classified information.

10.3.1 Ensure timely notification of personnel identified for a Periodic Reinvestigation (PR) and assists them with completing appropriate forms and entering the date into Electronic Questionnaire Investigations Processing (E-QIP) or the Electronic Personnel Security Questionnaire (EPSQ). Maintain the EPSQ on selected computers for personnel to update their clearances.

10.3.2. The SM will ensure that the AF Form 2583, Request for Personnel Security Action, DD Form 1879, DoD Request for Personnel Security Investigation, if required E-QIP or EPSQ are completed and free of errors prior to security package processing by the host base.

10.4. If the commander believes a condition exists that may affect the security eligibility of an individual, a recommendation will be to the host base ISPM to establish a SIF. The request must be fully justified and supported by clear rationale based on facts in the case.

10.5. Prescribed Forms: None.

10.6. Adopted Forms:

AF Form 2583, *Request for Personnel Security Action*

AF Form 2586, *Unescorted Entry Authorization Certificate*

AF Form 3137-*General Purpose* (11”x 8 ½”)

AF IMT 847, *Recommendation for Change of Publication*

DD Form 1879, DOD *Request for Personnel Security Investigation*

DD Form 2501, *Courier Authorization (Accountable)*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 704, *Secret* (Cover Sheet)

SF 705, *Confidential* (Cover Sheet)

SF 706, *Top Secret* (Label)

SF 707, *Secret* (Label)

SF 708, *Confidential* (Label,

JOHN C. FOBIAN, Brig Gen, USAFR
Commander, 433 Airlift Wing

Attachment 1
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-401, *Information Security Management Program*, 1 November 2005

AFI 31-401/AFRC Supp1, *Information Security Program Management*, 15 May 2007

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 31-4, *Information Security, Air Force Instruction*, 1 September 1998

DoD 5200.1-R, *Information Security Program*, 14 January 1997

T.O. 00-20F-2, *Inspection and Preventative Maintenance Procedures for Classified Storage Containers*, 6 March 2007

Abbreviations and Acronyms

ADLS- Aeronautical Data Link System

AETC- Air Education and Training Command

AF- Air Force

AFB- Air Force Base

AFI-Air Force Insurucuction

AFMAN-Air Force Manual

AFPD- Air Force Policy Directive

AFRC- Air Force Reserve Command

AIS- Automated Information Systems

ARPC- Air Reserve Personnel Center

AW- Airlift Wing

CC- Commander

CES- Civil Engineer Squadron

CF- Communications Flight

CF/SCB – Communications Flight/Information Systems Flight

CP-Command Post

DD- Department of Defense

DOD- Department of Defense

DSMPM- Personal Office

E-Mail- Electronic Mail

EPSQ- Electronic Personnel Security Questionnaire

E-QIP-Electronic Questionnaire Investigations Processing

GCCS- Global Command Control Systems

GSA- General Services Administration

GS- Grade Skill Level

HQ- Headquarters

ID- Identification

IMT-Information Management Tool

ISP- International Security Program

ISPM- Information Security Program Management

JPAS- Joint Personnel Adjudication System

NATO- North Atlantic Treaty Organization

NCO- Non-Commissioned Officer

OCA- Original Classification Authority

OI-Operating Instruction

OPM- Office of Personal Management

OPR- Office of Primary Responsibility

OPSEC- Operation Security

PR- Periodic Reinvestigation

PSI- Personnel Security Investigation

RDS- Records Disposition Schedule

SF-Standard Form

SCB- Information Systems Flight

SFS/SFA- Security Forces Squadron/ Security Forces Administration

SFS/S5B- Security Forces Squadron/ Pass and Registration Section

SFS/S5IP- Security Forces Squadron/ Personal and Information Security Section

SIF- Security Information File

SM- Systems Manager

TO-Technical Order

TSCO- Top Secret Control Officer

TX- Texas

UMD- Unit Manpower Document

USAFR- United States Air Force Reserve

UTA- Unit Training